Cloud-managed Security

Network security is essential for business integrity — and at the same time a complex topic: The increasing number of cyber attacks on companies and public institutions require a dynamic security concept that can react to new types of threats. Despite a state-of-the-art security architecture, isolated misconfigurations of deployed devices can result in major security gaps. With cloud-managed security you simplify the setup and secure your network professionally with little effort.

In this paper, you will learn how to set up security profiles for all devices of a network centrally via the LANCOM Management Cloud (LMC) and which security architecture is suitable for your deployment scenario.

What is cloud-managed security?

Cloud-managed security is when security functions are abstracted from the hardware, e.g. firewalls, and shifted to a software level. The security infrastructure is thus monitored and controlled on a virtualized basis. A management system that administers the functions securely and centrally can be the LANCOM Management Cloud (LMC), for example.

Cloud-managed security with the LMC — automated. secure. centralized.

With the LANCOM Management Cloud (LMC), you can manage, control, and optimize your entire network architecture in the areas of WAN, LAN, WLAN, and security. In combination with the LANCOM R&S®Unified Firewalls or the LCOS-based routers and SD-WAN gateways, you can activate security functions with just a few clicks for guaranteed reliable protection of networks, devices, and data. Developed in Germany and equipped with state-of-the-art Unified Threat Management (UTM) functions, the LANCOM R&S®Unified Firewalls offer, for example, maximum security and integrity for your HTTPS connections via SSL inspection. With the help of a content filter, content that is harmful to minors as well as to business can be blocked reliably.

And that's not all: Application management lets you control application usage on your network. Because you know best which applications you trust and which you want to prevent. Block specific individual applications or groups of applications. Route applications you specify, such as Microsoft Office 365, directly to the Internet (Local Internet Breakout) or to an external remote site.

As an additional security feature, the LMC handles the automatic establishment of VPN connections between all sites (Auto-VPN) and networks (end-to-end VLAN transmission, LANCOM Advanced Routing & Forwarding).

You can keep an eye on all these security capabilities in the menu under 'Security'. The following step-by-step guide will help you set up and configure the necessary security profiles in the LMC.

Setting up cloud-managed security in the LANCOM Management Cloud (LMC)

Perform the following steps to enable security settings in the LMC:

1. Log in to the LMC.
2. Check if the **SD-WAN** feature is active in the **Project specifications > SDN**.

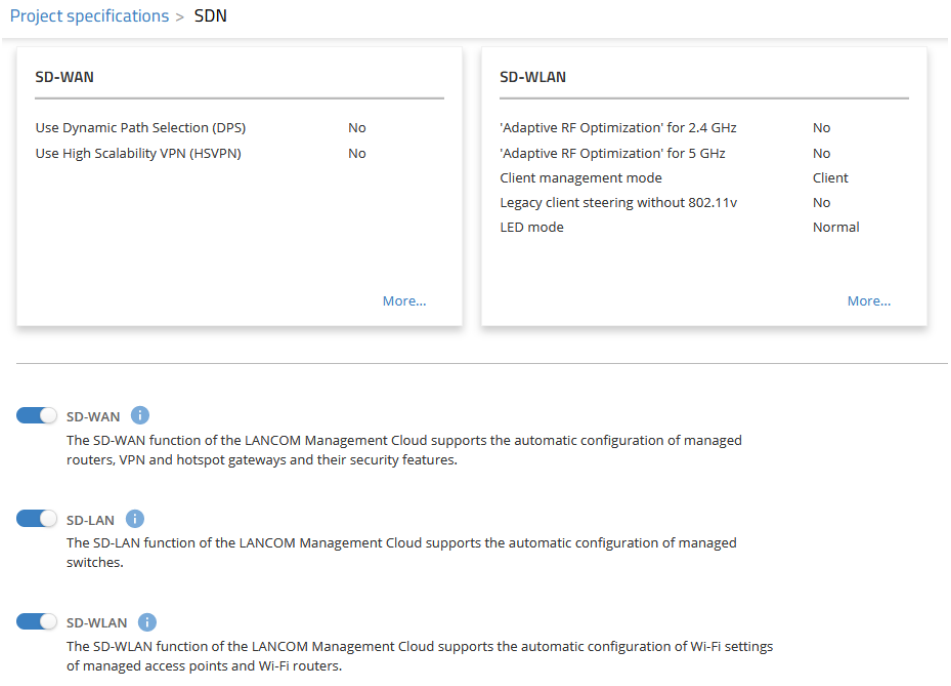

Figure 1: Project specifications > SDN

Activate **SD-WAN** if necessary. An additional 'Security' entry will then appear in the menu.

To use these functions, each device requires its own license! For LANCOM R&S®Unified Firewalls this is a Full License, for LCOS-based routers and SD-WAN gateways the LANCOM Content Filter option. These must be manually installed on the devices in advance.
One LMC license must also be active in the LMC for each device.

3. Under **Security > Profiles**, a security profile with default settings is automatically created for each network. In the overview, you can keep an eye on the security capabilities that have been set.

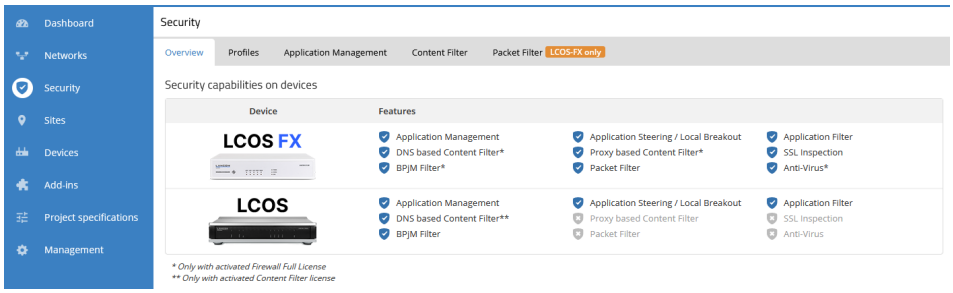

Figure2:
Overview of security capabilities

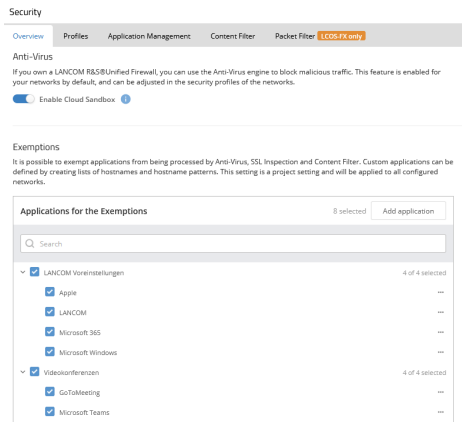

Figure 3:
settings of the security profiles

If necessary, enable the use of the **Cloud Sandbox**.
The Cloud Sandbox extends the anti-virus protection and is only active on networks where the anti-virus protection is active. To protect against threats that are not yet known, the LANCOM R&S®Unified Firewall can upload suspicious files to a protected cloud. In this separate environment, they are safely and reliably tested using Machine Learning and Sandboxing. Find out more in our Avira Protection Cloud infopaper.

If you enable the Cloud Sandbox, then the **Machine Learning features** will also be enabled.

Check the exception lists to see if a service still needs to be entered or deselected for your network.

4. You can now create and adjust rules globally for all networks in the **Application Management**, **Content Filter** and **Packet Filter** tabs according to your needs. You can later apply these to your networks / security profiles.

   - **Application Management** tab

   We distinguish between three categories in application management:

LCOS (Blue)	LCOS-based devices (routers and SD-WAN gateways) such as LANCOM 1926VAG
LCOS FX (Orange)	LANCOM R&S®Unified Firewalls
LCOS & LCOS FX (Green)	LCOS-based devices (routers and SD-WAN gateways) and LANCOM R&S®Unified Firewalls

   With this information you can check which service is detected by your device.

   You can either block or steer the traffic:

   i) **Block traffic**

   You can block the traffic such as to “Facebook” very easily for a network: Select the **Block traffic** checkbox in the upper area of Application Management. Then click the **Create new rule** button and in the new dialog that appears you can select one or more services.

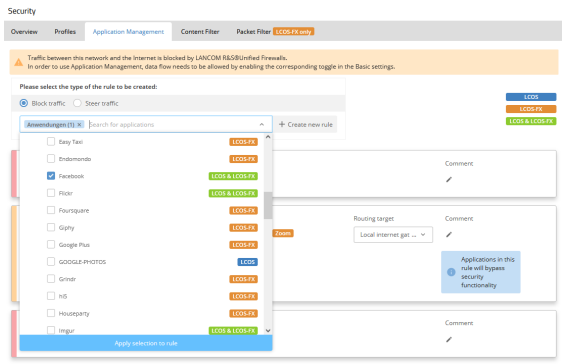

Figure 4:
Block traffic

   Apply your selection via the **Apply selection to rule** button. A created rule will be activated by default.

In this network, incoming and outgoing data traffic to the Internet is currently blocked by LANCOM R&S®Unified Firewalls. To use Application Management, you must first allow data traffic by setting the **Allow traffic from this network to the Internet (LANCOM R&S®Unified Firewall)** option. You do this in the basic settings of a security profile mentioned before.

ii) Steer traffic

In the upper area of Application Management, select the **Steer traffic** checkbox.

You can redirect the traffic such as to the conference service “GoToMeeting” very easily for a network, for that click the **Create new rule** button and in the new appeared dialog you can select one or more services.

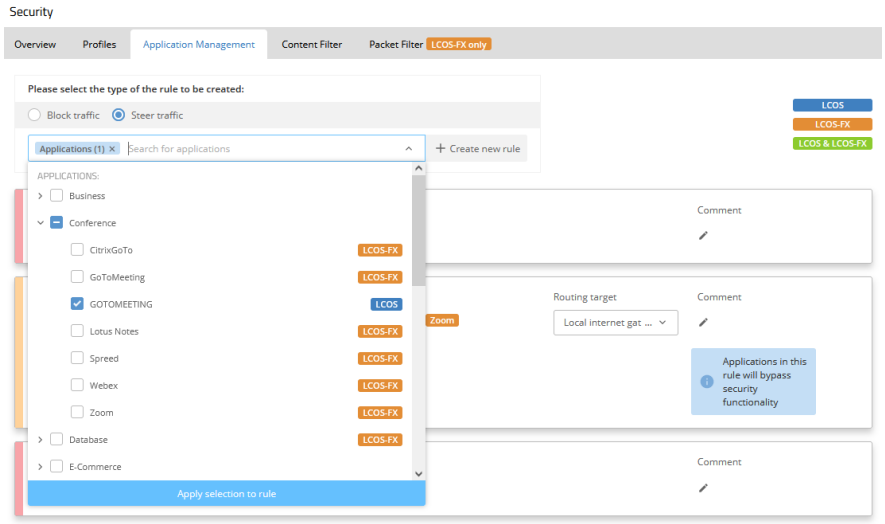

Figure 5:
Steer traffic

You need to decide how you want to redirect the traffic. You can do this in the **Routing target** drop-down menu.

For example, if you have selected for a network that all traffic is to be routed via the Central Site Gateway, you can have individual applications routed directly via an existing local Internet access (Local Internet Breakout).

- **Content Filter** tab

In this section, you can set the Content Filter rules for both the LANCOM R&S®Unified Firewalls and LCOS-based routers and SD-WAN gateways. As an example, we have provided you with a “Default Content Filter rule”. In order for you to test our example rule, you would only need to activate it.

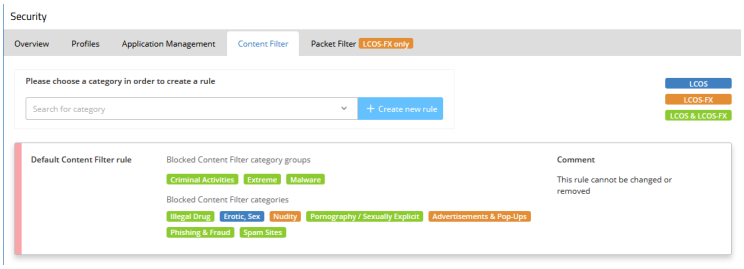

Figure 6:
Content Filter tab

- **Packet Filter** tab

In this section you can create packet filter rules that can be used in a security profile. First select an action (drop or accept) and a traffic direction (outgoing, incoming, or bidirectional). In the „Destination“ field you can define one or more destinations for the traffic, e.g. general targets like „Internet“ or „Any target“ or specific networks. The source of the traffic is automatically determined by the security profile in which you use this rule. In the last step, you can further refine the rule by specifying protocols and port numbers. Comma-separated enumerations and hyphenated network ranges are possible; however, these should not overlap.

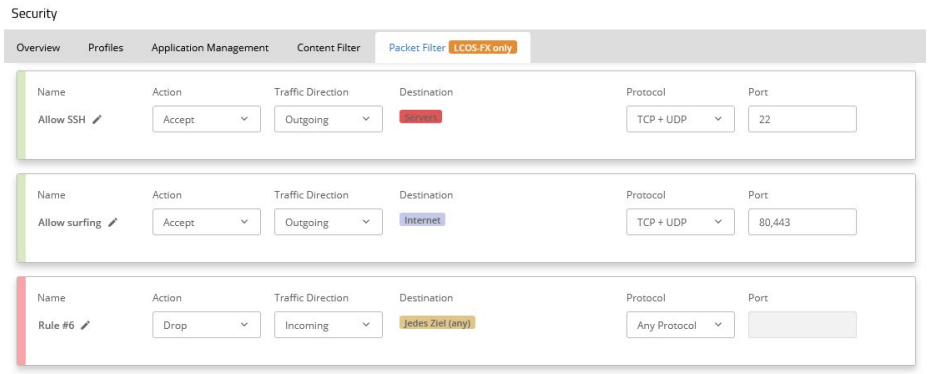

Figure 7:
Packet Filter tab

- **Basic settings**

You can reach the basic settings of a security profile by clicking on the corresponding name of your network under **Security > Profiles**.

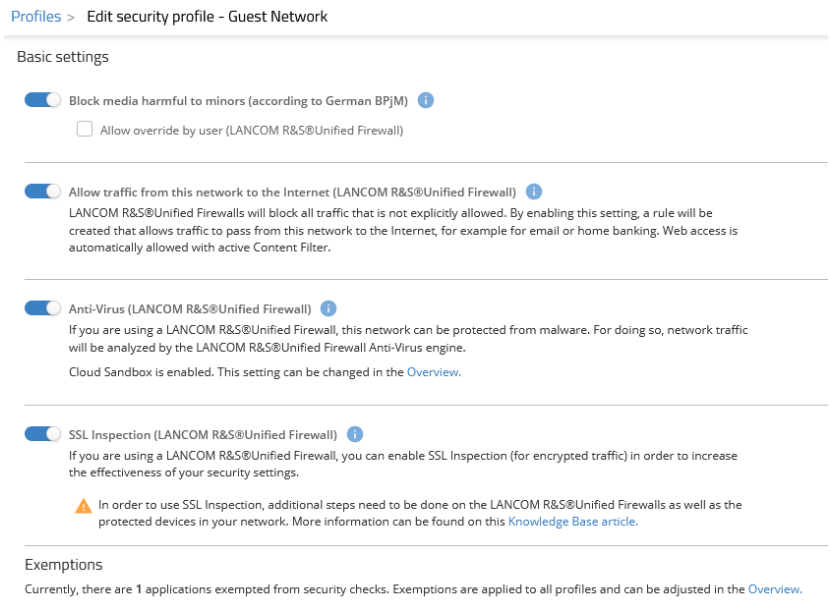

Figure 8:
Basic settings

i) **Block media harmful to minors (according to German BPjM)**
This option activates the LANCOM BPjM filter as a Content Filter with an official website list of "Bundesprüfstelle für jugendgefährdende Medien" (German Federal Review Board, BPjM). This filter list blocks domains whose content is officially classified as harmful to minors.

ii) **Allow traffic from this network to the Internet (LANCOM R&S®Unified Firewall)**
This option allows full access to the Internet (Pass-All). Alternatively, you can perform a more detailed configuration via the web interface of the LANCOM R&S®Unified Firewall.

iii) **Anti-Virus (LANCOM R&S®Unified Firewall)**
Traffic between this network and the Internet can be routed through the anti-virus engine of the LANCOM R&S®Unified Firewalls to detect and block suspicious files before they enter your network. In order to be able to check encrypted data traffic as well, SSL Inspection must also be activated and set up.

iv) **SSL Inspection (LANCOM R&S®Unified Firewall)**
If you have a LANCOM R&S®Unified Firewall, you can activate SSL Inspection to also control encrypted data traffic and thus increase the effectiveness of your security settings.

UTM features such as Anti-Virus and Content Filter require SSL Inpection. If SSL Inspection is active in the LANCOM R&S®Unified Firewall, the LANCOM R&S®Unified Firewall redirects HTTPS connections to itself and acts as a proxy between the end device and the server. The end device must explicitly accept this by trusting the Proxy Certificate Authority of the LANCOM R&S®Unified Firewall.

Necessary manual setup of certificates on the LANCOM R&S®Unified Firewalls during SSL inspection

If there are multiple LANCOM R&S®Unified Firewalls at multiple sites, there are two options:

a) CA per firewall: Each LANCOM R&S®Unified Firewall has an independent proxy certificate authority.
b) Company-wide CA: If an end device trusts a previously created and superordinate CA, it can be used at all sites without further effort.

Both cases are described in our Knowledge Base article, and LMC already takes care of some of the steps described there. However, there is still the installation of the certificates, which has to be done manually.

5. You can view the security functions you have set for each security profile, i.e. for each of your networks, under **Security > Profiles**.

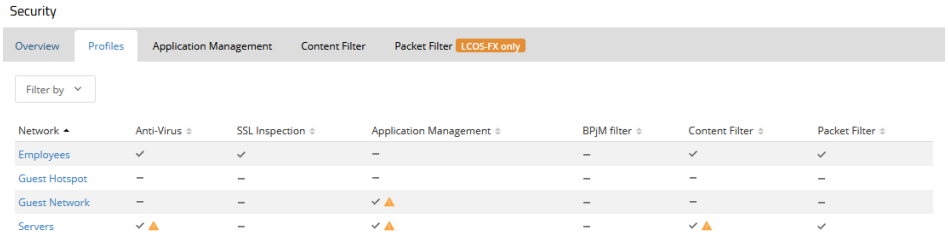

Figure 9:
Security profiles

Exemplary application scenarios

A security infrastructure should be specifically adapted and tuned to your company size and the workload of your network in order to adapt security requirements to your needs. This results in the following three scenarios:

Scenario 1: Decentralized security at all sites

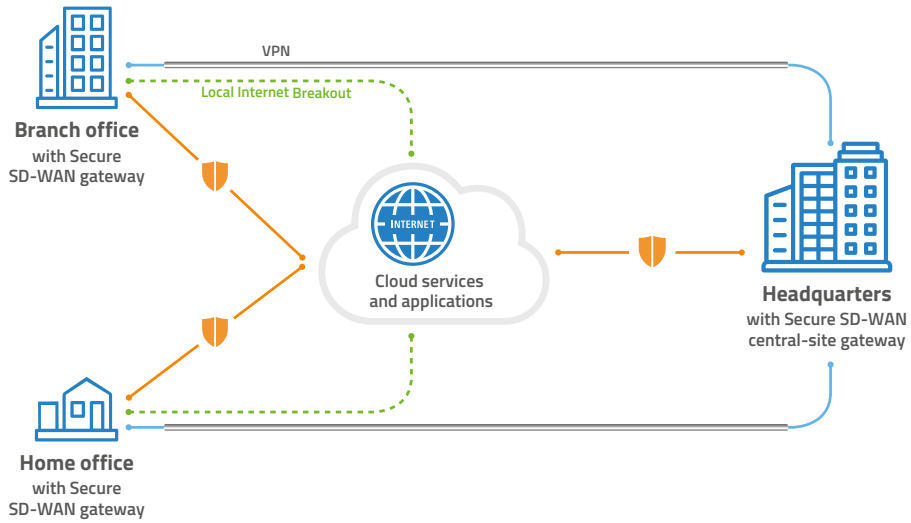

Figure 10:
Scenario 1: Decentralized security at all sites

In this scenario, all branch offices are connected to the headquarters via SD-WAN / Auto-VPN for secure access to centrally hosted resources and services. A gateway with fully activated security functions is applied at each site, which means that the security requirements are defined individually for each site. In addition, latency for users is kept very low due to a Local Internet Breakout of trusted cloud-based applications. This scenario should cover most standard cases.

Recommendation: Deploy a local LANCOM R&S®Unified Firewall at each site. This allows you to achieve maximum performance through local Internet access while maintaining a high level of security through the firewall.

Scenario 2: Centralized security

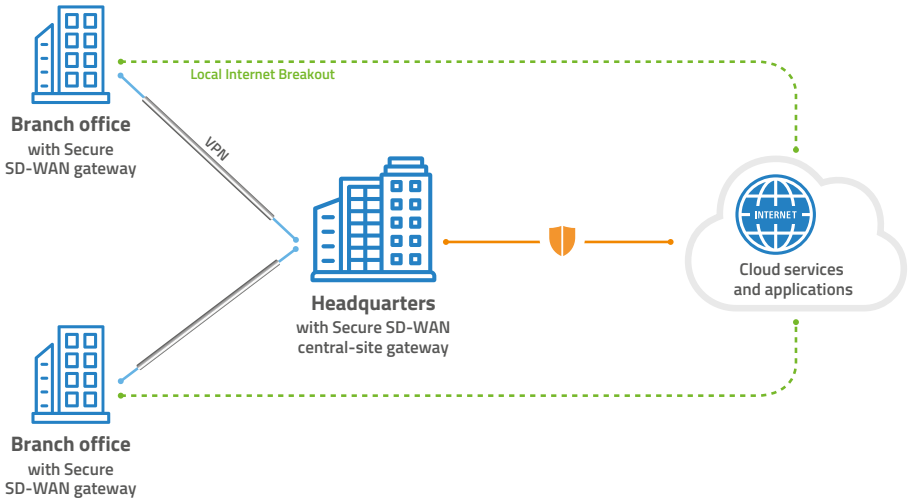

Figure 11:
Scenario 2:
Centralized security

This scenario is ideal and cost-effective for smaller site networking scenarios. Here, just as before, all branch offices are connected to the headquarters via SD-WAN / Auto-VPN for secure access to centrally hosted resources and services. A high-performance gateway with fully activated security functions is applied in the headquarters, which defines the security requirements for all branch offices. In the branch offices, it is sufficient to apply smaller SD-WAN gateways without activated security functions, whereby a Local Internet Breakout for trusted cloud applications can reduce the traffic load in the headquarters.

This scenario is particularly suitable for cases in which local Internet access plays a subordinate role or is not required, for example, if machines are to be connected at the respective locations.

Scenario 3: Small networks — Equal sites without headquarters

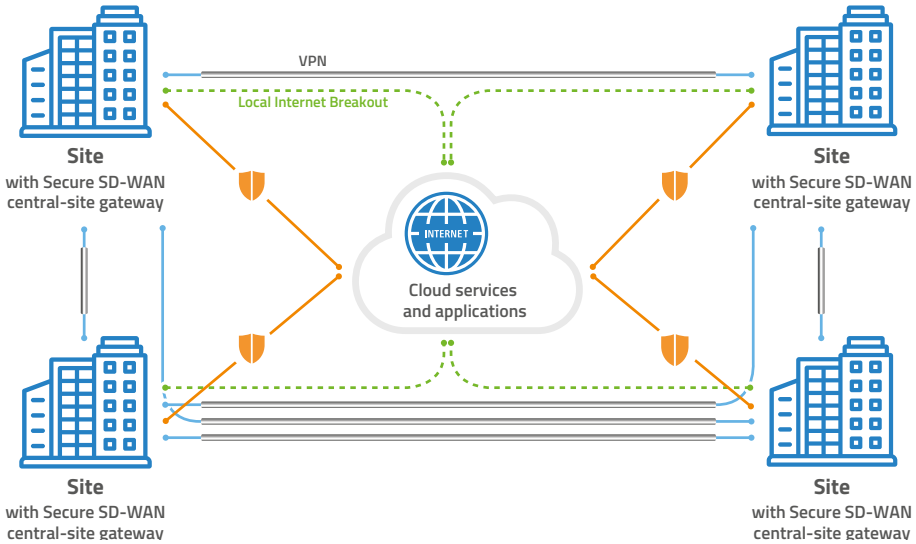

Figure 12: Scenario 3: Small networks — Equal sites without headquarters

In the case of company networks without a classic headquarters, all locations are completely interconnected with each other via Auto-VPN. A gateway with activated security functions is applied at all sites. The sites each have equal access to locally hosted services. Here, just as before, the security policies can be defined individually for each site, as can the Local Internet Breakout for trusted cloud applications.

LANCOM Systems GmbH
Adenauerstr. 20/B2
52146 Wuerselen | Germany
info@lancom.de
www.lancom-systems.com