Key considerations for the Federal Zero Trust strategy and what it means for your agency

zscaler™

Defining Zero Trust

Like most great ideas, the concept of zero trust (ZT) is refreshingly simple: allow only authorized users access to an application. How hard can that be? It turns out, it's much harder than some might have thought—until now. In this paper, we'll review the historical precedent, implementing what you can with contemporaneous tools, and why zero trust principles are orthogonal to the current state of security. And finally, the paper will outline what you can do to better prepare for the ZT tsunami.

With Executive Order 14028, zero trust went from a trending technology buzzword to a series of concrete tasks that must be implemented in a matter of months. The good news is that there are zero trust architectures that exist today. The bad news is that there is a plethora of architectures to choose from: DOD, NIST, CISA, and FISMA to name a few. As the saying goes "The good thing about a standard is that there are so many to choose from!"

But the key point is that no one vendor, whatever the claim, can deliver a turn-key zero trust model. It's not possible simply because there is no one vendor that has the capability and presence in end point (GFE), network, security, application, database, and cloud/SaaS. Agencies should focus on casting a wide net to provide as much protection as possible in the shortest amount of time. Once the protective net is in place, surgical changes can increase the levels of protection.

Before we get into what zero trust means, a quick primer on the history is required. In the past, Network Access Control (NAC) was all the rage. It ensured that the end host (GFE) had the proper protection (Antivirus, Authentication, patches etc.) before it gained access to the network. This was a time when a virus would spread throughout an organization via infected computers. Some vendors also included, or tried to, end-to-end encryption to protect the valuable traffic. Network World summed it up, if somewhat scathingly, as "Five years of hype, buzzwords, white papers, product launches, standards battles and vendor shakeouts have resulted in very little in the way of clarity."[1] These were not small companies battling in the NAC arena. Marquee names such as Cisco, HP, Microsoft, Juniper, McAfee, and Symantec were all vying to be the king of the NAC hill. A venerable who's who of technology all failed to deliver on the promise of better security.

The reason for the epic failure can be found in the name: Network Access Control. Network was built from the ground-up to connect all endpoints with the least number of bottlenecks. Ethernet was designed to ensure unfettered access to the network and purposely eliminated prioritization or scheduling. Trying to protect the network with NAC was no different than asking the toll booth collectors of every highway to inspect every car for contraband—a quixotic task if ever there was one.

So what steps are required to cast a wide net? Do you do it by volume of traffic? The number of users? The topology of the network? You might hear a network jockey say, "We can do it at the headend." "We can put a WAF[2] and deal with it," an app person might say. "I'll upgrade my proxy to get ready," or you might hear from the security team, "We'll really need to beef up the VPN and try to get the split tunnel right".

Steps to Approaching the Zero Trust Strategy

The ZT truth is that appliances and networks are exactly the wrong places to enforce anything. NAC is a painful reminder of the futility of this approach—asking the network and appliances to enforce ZT. So, what is the right approach? Let's dig in!

1. Identify the critical applications: I don't mean the greatest number of users, top talkers by IP address, or number of times a user logs into an application. Identify the applications that will shut down your organization if it is compromised. This can only come from the top down. So, if you don't have an architectural council, get busy creating one. C-Suite can provide the necessary direction, but the architects council can provide the level of detail required. Do keep in mind that the network is precisely the wrong place to identify what is critical. Network-based information can only give you volumetric information, not the criticality of that application.

2. Gather who's talking to whom from the network. "But you just said the network is the wrong place to gather this information!" This exercise is to gather the information of top talkers once the critical applications have been identified. You need to know where to throw the wide net to protect yourself. Think of this step as using a sonar to find where the schools of fish are. Every router can provide conversation information by using Netflow. If you don't have a Netflow collector, you can just collect the information from the router's command line and collate the information.[3]

3. Once you have identified the top talkers of the critical applications, it's time to identify the users associated with those IP's. This information can be gathered from the application log, Active Directory, proxy, SIEM, DHCP, LoadBalancer, and other logs. It sounds daunting, but because you have the IP address to join the information, confirming the actual user is just a pivot table away.

4. Your GFE or endpoint management solution can then report on the readiness of the GFE to connect. Zero trust starts with the device posture. So, be sure to set a baseline for what patches will be required for the GFE. One note of caution: If your users have been off-premises for an extended period, be mindful of how many users you ask to return on a given day. The sheer number of updates and patches can easily overwhelm the TIC/Internet access. Again, this is an area that a ZT solution can address with secure Direct to Internet options.

5 "But what about the Internet, isn't that the most important place to start?" Surprisingly, the answer is no. In most cases, zero trust is providing a user-to-application-level permission for on-premises and private cloud based applications. But, of course, the Internet must be accounted for. Zscaler can be that circuit breaker for all SaaS, IaaS, Cloud, social media and recreational internet applications. Zscaler is always on guard to stop suspicious activity.[4]

6 "My VPN is going strong…" Shoring up what you have is the natural reaction, especially when time to completion is a critical factor. Unfortunately, VPN is one of the biggest offenders of ZT principles. Here's a simple litmus test: if any appliance works at the level of IP address, TCP/UDP ports, or IP based access-lists (ACL) it is **not** zero trust.

As you may have noticed with the above steps, you will be well on your way to addressing all five pillars of the Federal zero trust Strategy and CISA's Zero Trust Maturity Model.[5]

1	2	3	4	5
IDENTITY	**DEVICES**	**NETWORKS**	**APPLICATIONS AND WORKLOADS**	**DATA**
Agency staff use enterprise-managed identities to access the applications they use in their work. Phishing-resistant MFA protects those personnel from sophisticated online attacks.	The Federal Government has a complete inventory of every device it operates and authorizes for Government use, and can prevent, detect, and respond to incidents on those devices.	Agencies encrypt all DNS requests and HTTP traffic within their environment and begin executing a plan to break down their perimeters into isolated environments.	Agencies treat all applications as internet-connected, routinely subject their applications to rigorous empirical testing, and welcome external vulnerability reports.	Agencies are on a clear, shared path to deploy protections that make use of thorough data categorization. Agencies are taking advantage of cloud security services to monitor access to their sensitive data and have implemented enterprise-wide logging and information sharing.

Remember, zero trust is not the finish line. It's a continual maturation of organizations' cyber practices. While there is no easy-button or end-to-end zero trust turn-key solution an agency can go out and buy, Zscaler can be that wide net to provide the highest level of ZT protection in the shortest time frame. Over 100 government agencies and federal integrators depend on Zscaler today and we are the only DOD Impact Level 5 approved solution. It's no wonder that 8 of the top 10 financial institutions, 6 of the top 10 Aerospace & Defense companies, and 7 of the top 10 conglomerates all chose Zscaler as its SASE and ZT solution. Visit **zscaler.com/federal** to learn more.

Appendix A

Netflow output from a router showing top applications and conversation pairs.

```
AnyRouter#show ip cache flow
! deleted for brevity
  Protocol       Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
  --------       Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-WWW      189939431     44.2        29   836   1294.9       4.9       7.3
TCP-SMTP        66401      0.0       129   802      1.9       3.4       6.1
TCP-X          176941      0.0        57   159      2.3      31.1       6.7
TCP-BGP        425389      0.0        89    50      8.8      92.7       1.1
…
IP-other       431228      0.1        21   216      2.1      54.6       2.6
Total:      2208585558    514.2        17   605   9234.2       3.9       9.6

SrcIf         SrcIPaddress    DstIf        DstIPaddress      Pr SrcP DstP    Pkts
Gi0/2         172.16.172.63   Hs3/0        172.168.224.163   06 01BB 04C4     1
Gi0/2         172.16.172.63   Hs3/0        172.168.224.163   06 01BB 04C6     3
Hs1/0         10.16.121.30    Gi0/2        172.183.33.30     06 04E7 46A0     4
Gi0/2         172.16.172.63   Hs3/0        172.168.224.250   06 01BB 075A     1
Hs3/0         172.168.140.23  Gi0/1        172.194.251.47    06 01BD 0FBA     1
Gi0/1         172.16.172.63   Hs3/0        172.168.224.124   06 01BB 0670     2
Gi0/1         172.16.172.63   Hs3/0        172.168.224.124   06 01BB 0671     1
Gi0/2         172.16.172.132  Hs3/0        172.168.224.111   06 01BB 0708    70
Gi0/2         172.16.172.132  Hs3/0        172.168.224.111   06 01BB 0707    70
Hs1/0         172.18.87.35    Gi0/2        172.194.251.35    06 100A 3E91     3
Hs3/0         172.168.136.98  Gi0/2        172.183.28.62     06 0622 2261     1
Gi0/1         192.172.245.48  Hs3/0        172.168.217.211   06 0050 0698    99
Gi0/1         172.32.128.243  Local        10.157.17.4       06 00B3 E932    26
Hs1/0         10.16.121.132   Gi0/1        10.16.108.37      06 0404 1775     1
Hs3/0         172.168.136.22  Gi0/2        172.183.28.62     06 071A 2261     2
Hs1/0         10.16.121.4     Gi0/1        10.16.108.37      06 0404 1775     1

!deleted for brevity
AnyRouter#
```

Sources

[1] https://www.networkworld.com/article/2209345/nac--what-went-wrong-.html

[2] Web Application Firewall

[3] See Appendix A for an example of a Cisco router based Netflow report. Every router vendor supports a similar command.

[4] 2 Billion malware was protected by Zscaler in January 2022, and over 34 billion attacks were stopped in 2021.

[5] https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

About Zscaler

Zscaler accelerates digital transformation with its Zero Trust Exchange, a SASE-based platform that provides fast, secure connections between users, devices, and applications over any network. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com