VITAL CYBER

MCNC's Managed Firewall Service

MCNC's Managed Firewall service is built to solve your toughest cybersecurity challenges.

Welcome & Agenda

VITAL CYBER

1. **Introductions**
2. **What Is MCNC's Managed Firewall Service?**
   - Managed Security Approach
   - Service Enhancements
   - Other Service Specifics
3. **What To Expect**
   - Service Level Targets
   - Sign Up for Migration/Enrollment
   - Onboarding Scheduled
   - Onboarding Process
4. **Q&A**

Introductions

VITAL CYBER

Ruthy Mabe

Sr. Manager, Security Services

Chris Beal

VP, Cybersecurity Initiatives & CISO

Dave Furiness

Sr. Director Network Consulting & K-12 Advocate

David Brain

Director, Systems & Cybersecurity Operations

Gonz Guzman

Lead Client Network Engineer

Service Enhancements

VITAL CYBER

Palo Alto Networks (PAN) Application-Level Firewall (NextGen Firewall)

- Moving from port-based firewall to application-level firewall
- APP-ID Tech Brief: https://www.paloaltonetworks.com/resources/techbriefs/app-id-tech-brief.html

Advanced Security Service

- Advanced Threat Prevention License: https://www.paloaltonetworks.com/network-security/advanced-threat-prevention
- Post deployment FW hardening / policy optimization
- Annual proactive security configuration review
- Proactive outreach concerning observed activity or issues related to security events

Change Management & Risk Assessment

- Configuration changes submitted by PSU reviewed for potential security and performance impacts
- Potential concerns documented and reviewed with authorized PSU personnel prior to change

Service Level Agreement with Established Change Management Windows

- Standard Changes submitted prior to 12pm on Business Days should be included in that day's window (3:00 pm - 6:00 pm) on a reasonable effort basis

Centralized Logging

- 60 days of NGFW Event Logs stored off-site from PSU premise and available for review by PSU via Palo Alto Networks Panorama Platform.

Other Service Specifics

VITAL CYBER

Contracted bandwidth determines Palo Alto Networks model deployed

Bandwidth Tier	PAN NextGen Model
< 1 Gbps	**PA-440**
1 - 2 Gbps	**PA-460**
3 - 4 Gbps	**PA-3410**
5 - 10 Gbps	**PA-3440**
15 - 20 Gbps	**PA-5420**
30 - 40 Gbps	**PA-5450**

NCREN bandwidth upgrades may include a PAN FW upgrade as appropriate

Fully-managed and monitored by MCNC's Security Operations team

- The same team delivering MCNC's Managed Endpoint Protection service
- A PSU self-managed service offering is not currently available but is under consideration.

24x7x365 Proactive Monitoring, Administration, & Support Services

- PSUs will continue to contact MCNC as before: Ticket, Email, Phone

SLA Targets: *Incident Support*

Definition: A service impacting, or potentially service impacting issue that requires investigation and or intervention. This may include incidents impacting the normal operations of the service (**operational incidents**) or security alerts that require review and response by the operations team (**security incidents**).

Incident Priority Level	Description
P1 / Critical	**Operational**: Systems at one or many PSU sites are completely unavailable. Significant business impact. **Security**: Security alert or detected anomaly with a high potential to cause significant damage to critical assets.
P2 / High	**Operational**: Systems at one or many PSU sites are partially unavailable. Some business impact. **Security**: Security alert or detected anomaly with a potential for widespread impact.
P3 / Medium	**Operational**: Operational performance of PSU sites remains normal and business operations are not impacted, but a fault in the service has been identified and a resolution is required. **Security**: Security alert or detected anomaly that is potentially malicious but not known to be targeted or widespread.
P4 / Low	**Operational**: The PSU's core business is unaffected and the issue is informational in nature. **Security**: Security alert or detected anomaly that is low-risk and low-impact

Incident Priority Level	Response Time
P1 / Critical	4 hours or less, 24 hours a day, 7 days a week, 365 days a year.
P2 / High	24 hours or less, 24 hours a day, 7 days a week, 365 days a year.
P3 / Medium	3 days or less Business Days
P4 / Low	7 days or less Business Days

SLA Targets: *Change Requests*

Definition: A request to modify an existing service configuration (Move/Add/Change/Delete)

Introducing Change Management Window*: 3pm-6pm Eastern - Standard Changes submitted prior to 12pm on Business Days may be included in that day's window on a reasonable effort basis.

Incident Priority Level	Description
Standard Change	A *low-risk change* that is implemented via a procedure that has been previously defined and tested. Example: security or NAT policy addition.
Normal Change	All other changes that have not been previously defined and tested. As such, these changes are deemed to be *higher-risk* and require additional vetting.
Urgent Change	Standard or Normal changes that cannot meet established daily change management window* or lead times
Emergency Change	A change that must be implemented as soon as possible in response to an incident.

Incident Priority Level	Response Time
Standard Change	Standard changes will be implemented within 1 Business Day from the time the request is submitted until the time that it is implemented, during the daily change management window. PSU can call in request to expedite
Normal Change	Normal changes will be implemented within 5 Business Days, during the daily change management window, and design and risk analyses will be performed.
Urgent Change	Urgent changes are project-driven, and may be implemented outside of established daily change management window with approved business justification, design and risk analyses. 24 hours a day, 7 days a week, 365 days a year. Must be called in.
Emergency Change	Emergency changes will be implemented as soon as possible in conjunction with the resolution of the associated P1 to P4 Incident, 24 hours a day, 7 days a week, 365 days a year. Must be called in.

Sign Up for Migration/Enrollment

All NCDIT Cisco Firewalls will be migrated over the coming months

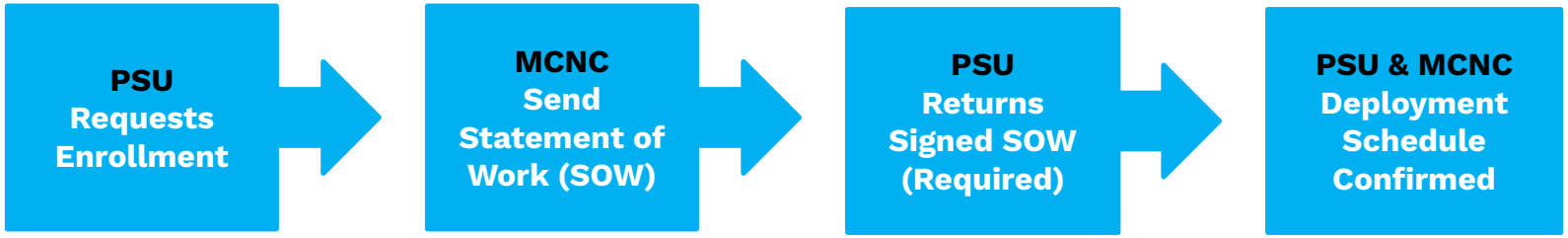
Existing NCDIT Cisco Firewall Users - Migration

SOW will be sent by MCNC starting the week of September 19, 2022

- Will include link to informational webinar and FAQ info

New Subscribers should request enrollment via securityservices@mcnc.org

New Firewall Subscribers Enrollment



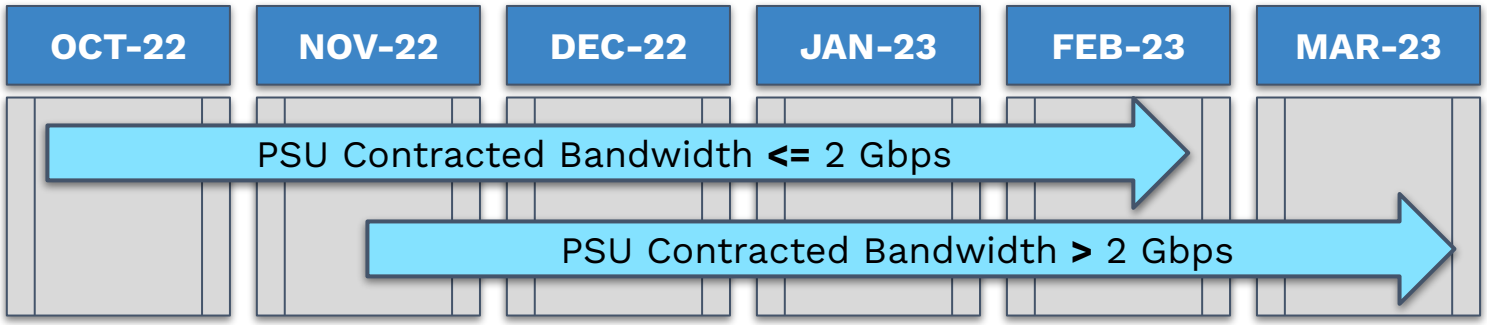
Onboarding Process Summary

VITAL CYBER

No.	Stage	Owner	Notes
0	**PSU Signs SOW**	MCNC Service Management & PSU	All PSUs are required to agree to a no-cost statement of work
1	**Firewall Provisioning**	MCNC Client Network Engineering & Network Management	Migrate the configuration from the DIT ASA firewall to Palo Alto Networks. Apply base level configuration to the PAN FW. Provision the FW for management and log retention in Panorama
2	**Scrub Phase**	MCNC Security Engineering	MCNC Security Engineering will run each provisioned firewall through a scrub phase before deploying.
3	**Risk Review**	Client Network Engineering & PSU	Documentation regarding identified weaknesses/risks will be provided to and reviewed with PSU for risk acceptance
4	**Deployment**	MCNC Service Management & Client Network Engineering	MCNC Project Manager will coordinate onsite installation with PSU and appropriate onboarding team
5	**Policy Optimization**	MCNC Security Engineering & PSU	MCNC may suggest new/revised sets of security policies based on analysis of the post-deployment firewall traffic logs.

Onboarding Scheduling Summary

Projected Project Schedule



Supply chain issues are resulting in long product lead times and some uncertainty

MCNC is working to expedite firewall deliveries for PSUs pending bandwidth upgrades > 2 Gbps. This is work in progress.

Each PSU engagement will last 2-4 weeks (excluding 30 - 60 day policy optimization work activity)

All cutovers will be performed after hours, with dates and times approved by the PSU

Questions?

VITAL CYBER

Thank You!

Contact Us:

securityservices@mcnc.org

Escalation Contacts:

Ruthy Mabe,
Manager, Security Services
rmabe@mcnc.org

Dave Furiness
K-12 Client Advocate
dfuriness@mcnc.org